To be published in proceedings of: ICCSA 2009 The 3rd International Conference on Complex Systems and Applications, University of Le Havre, France, June 29- July 02, 2009.

Chaotic Pseudo Random Number Generators via Ultra Weak Coupling of Chaotic Maps and Double Threshold Sampling Sequences.

René Lozi

Abstract—**Generation of random or pseudorandom numbers, nowadays, is a key feature of industrial mathematics. Pseudorandom or chaotic numbers are used in many areas of contemporary technology such as modern communication systems and engineering applications. More and more European or US patents using discrete mappings for this purpose are obtained by researchers of discrete dynamical systems [1], [2]. Efficient Chaotic Pseudo Random Number Generators (CPRNG) have been recently introduced. They use the ultra weak multidimensional coupling of *p 1*-dimensional dynamical systems which preserve the chaotic properties of the continuous models in numerical experiments. Together with chaotic sampling and mixing processes, ultra weak coupling leads to families of (CPRNG) which are noteworthy [3], [4].**

In this paper we improve again these families using a double threshold chaotic sampling instead of a single one.

We analyze numerically the properties of these new families and underline their very high qualities and usefulness as CPRNG when very long series are computed.

Index Terms—**Chaos, Discrete time systems, Floating point arithmetic, Random number generation.**

I. Introduction

Efficient Chaotic Pseudo Random Number Generators (CPRNG) have been recently introduced. The idea of applying discrete chaotic dynamical systems, intrinsically, exploits the property of extreme sensitivity of trajectories to small changes of initial conditions. They use the ultra weak multidimensional coupling of *p 1*-dimensional dynamical systems which preserve the chaotic properties of the continuous models in numerical experiments. The process of chaotic sampling and mixing of chaotic sequences, which is pivotal for these families, works perfectly in numerical simulation when floating point (or double precision) numbers are handled by a computer.

It is noteworthy that these families of very weakly coupled maps are more powerful than the usual formulas used to generate chaotic sequences mainly because only additions and multiplications are used in the computation process; no division being required. Moreover the computations are done using floating point or double precision numbers, allowing the use of the powerful Floating Point Unit (FPU) of the modern microprocessors (built by both Intel and Advanced Micro Devices (AMD)). In addition, a large part of the computations can be parallelized taking advantage of the multicore microprocessors which appear on the market of laptop computers.

In this paper we improve the properties of these families using a double threshold chaotic sampling instead of a single one. The genuine map *f* used as one-dimensional dynamical systems to generate them is henceforth perfectly hidden.

R. Lozi is with the Laboratory J. A. Dieudonné, UMR CNRS 6621, University of Nice Sophia-Antipolis, 06108 Nice Cedex 02, France and the Institut Universitaire de Formation des Maîtres Célestin Freinet-académie de Nice, University of Nice-Sophia-Antipolis, 89 avenue George V, 06046 Nice Cedex 1, France (corresponding author to provide phone: 04-93-53-75-08; e-mailrlozi@unice.fr).

II. Ultra Weak Multidimensional Coupling

A. System of p-Coupled Symmetric Tent Map

When a dynamical system is realized on a computer using floating point or double precision numbers, the computation is of a discretization, where finite machine arithmetic replaces continuum state space. For chaotic dynamical systems, the discretization often has collapsing effects to a fixed point or to short cycles [5], [6]. In order to preserve the chaotic properties of the continuous models in numerical experiments we have recently introduced an ultra weak multidimensional coupling of *p* one-dimensional dynamical systems which is noteworthy [7].

In this specific case we have chosen as an example the symmetric tent map defined by

$$f_a(x) = 1 - a|x| \quad (1)$$

with the value $a = 2$, later denoted simply as f, even though others chaotic map of the interval (as the logistic map) can be used for the same purpose. The dynamical system associated to this one dimensional map is defined by the equation on the interval $\mathbf{J} = [-1, 1] \subset \mathbb{R}$ [8].

$$x_{n+1} = 1 - a|x_n| \quad (2)$$

The system of *p*-coupled dynamical systems is then:

$$X_{n+1} = F(X_n) = A \cdot \left(\underline{f}(X_n) \right) \quad (3)$$

with

$$X = \begin{pmatrix} x^1 \\ \vdots \\ x^p \end{pmatrix}, \quad \underline{f}(X) = \begin{pmatrix} f(x^1) \\ \vdots \\ f(x^p) \end{pmatrix} \quad (4)$$

and

$$A = \begin{pmatrix} 1-(p-1)\varepsilon_1 & \varepsilon_1 & \cdots & \varepsilon_1 & \varepsilon_1 \\ \varepsilon_2 & 1-(p-1)\varepsilon_2 & \cdots & \varepsilon_2 & \varepsilon_2 \\ \vdots & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \vdots & \vdots \\ \varepsilon_p & \cdots & \cdots & \varepsilon_p & 1-(p-1)\varepsilon_p \end{pmatrix} \quad (5)$$

F is a map of $\mathbf{J}^{\mathbf{p}}$ into itself.

Several combinations can be given for the relative values of the ε_i, in this paper we choose

$$\varepsilon_i = i\,\varepsilon_1 \qquad i = 2, \ldots, p \quad (6)$$

The matrix A is always a stochastic matrix iff the coupling constants ε_i verify

$$0 \le \varepsilon_i \le \frac{1}{p-1} \quad (7)$$

When $\varepsilon_i = 0$ the maps are decoupled, when $\varepsilon_i = \frac{1}{p-1}$ they are fully cross coupled. Generally, researchers do not consider very small values of ε_i because it seems that the maps are quasi decoupled with those values and no special effect of the coupling is expected. In fact it is not the case and ultra small coupling constant (as small as 10^{-7} for floating point numbers or 10^{-14} for double precision numbers), allows the construction of very long periodic orbits, leading to sterling chaotic generators.

Moreover each component of these numbers belonging to $\mathbb{R}^p$ is equally distributed over the finite interval $\mathbf{J} \subset \mathbb{R}$. Numerical computations show that this distribution is obtained with a very good approximation. They have also the property that the length of the periods of the numerically observed orbits is very large [7].

B. Chaotic Pseudo-Random Generators

However chaotic numbers are not pseudo-random numbers because the plot of the couples of iterated points (x_n, x_{n+1}) in the phase plane reveals the map f used as one-dimensional dynamical systems to generate them.

Nevertheless we have recently introduced a family of Enhanced Chaotic Pseudo Random Number Generators (CPRNG) in order to compute very fast long series of pseudorandom numbers with desktop computer [9]. This family is based on the previous ultra weak coupling which is enhanced in order to conceal the chaotic genuine function.

In the aim of hiding f in the phase space $\left(x_n^l, x_{n+1}^l\right)$ two mechanisms are used. The pivotal idea of the first one mechanism is to sample chaotically the sequence $\left(x_0^l, x_1^l, x_2^l, \ldots, x_n^l, x_{n+1}^l, \ldots\right)$ generated by the l-th component x^l, selecting x_n^l every time the value x_n^m of the m-th component x^m, is strictly greater than a threshold $T \in \mathbf{J}$, with $l \neq m$, for $1 \le l, m \le p$.

A second mechanism can improve the unpredictability of the chaotic sequence generated as above, using synergistically all the components of the vector X, instead of two. This simple mechanism is based on the chaotic mixing of the *p-1* sequences $\left(x_0^1, x_1^1, x_2^1, \ldots, x_n^1, x_{n+1}^1, \ldots\right)$, $\left(x_0^2, x_1^2, x_2^2, \ldots, x_n^2, x_{n+1}^2, \ldots\right)$, …, $\left(x_0^{p-1}, x_1^{p-1}, x_2^{p-1}, \ldots, x_n^{p-1}, x_{n+1}^{p-1}, \ldots\right)$ using the last one $\left(x_0^p, x_1^p, x_2^p, \ldots, x_n^p, x_{n+1}^p, \ldots\right)$ with respect to a given partition T_1, T_2, …, T_{p-1} of $\mathbf{J}$, to distribute the iterated points.

C. Numerical Results

As an example we explicit both mechanisms taking *4*-coupled equations for (3). The value of x_n^4 commands the chaotic sampling and the mixing processes as follows.

Let us set three threshold values T_1, T_2 and T_3

$$-1 < T_1 < T_2 < T_3 < 1 \quad (8)$$

we sample and mix together chaotically the sequences $\left(x_0^1, x_1^1, x_2^1, \ldots, x_n^1, x_{n+1}^1, \ldots\right)$, $\left(x_0^2, x_1^2, x_2^2, \ldots, x_n^2, x_{n+1}^2, \ldots\right)$ and $\left(x_0^3, x_1^3, x_2^3, \ldots, x_n^3, x_{n+1}^3, \ldots\right)$ defining $\left(\overline{x_0}, \overline{x_1}, \overline{x_2}, \cdots, \overline{x_q}, \overline{x_{q+1}}, \ldots\right)$ by

$$\overline{x_q} = \begin{cases} x_n^1 & iff \quad x_n^4 \in \left]T_1, T_2\right[\\ x_n^2 & iff \quad x_n^4 \in \left[T_2, T_3\right[\\ x_n^3 & iff \quad x_n^4 \in \left[T_3, 1\right[\end{cases} \quad (9)$$

Numerical results about chaotic numbers produced by (3) - (9) show that they are equally distributed over the interval **J**.

In order to compute numerically an approximation of the invariant measure also called the probability distribution function $P_{\mathbf{N}}(x)$ linked to the *1*-dimensional map f we consider a regular partition of M small intervals (boxes) r_i of **J**.

$$\mathbf{J} = \bigcup_0^{M-1} r_i \quad (10)$$

$$r_i = [s_i, s_{i+1}[\;, \; i = 0, M-2 \quad (11)$$

$$r_{M-1} = [s_{M-1}, 1] \quad (12)$$

$$s_i = -1 + \frac{2i}{M} \quad i = 0, M \quad (13)$$

the length of each box is

$$s_{i+1} - s_i = \frac{2}{M} \quad (14)$$

All iterates $f^{(n)}(x)$ belonging to these boxes are collected (after a transient regime of Q iterations decided *a priori*, i.e. the first Q iterates are neglected). Once the computation of $N+Q$ iterates is completed, the relative number of iterates with respect to N/M in each box r_i represents the value $P_{\mathbf{N}}(s_i)$. The approximated $P_{\mathbf{N}}(x)$ defined in this article is then a step function, with M steps. As M may vary, we define

$$P_{M,N}(s_i) = \frac{1}{2}\frac{M}{N}(\#r_i) \quad (15)$$

where $\#r_i$ is the number of iterates belonging to the interval r_i and the constant 1/2 allows the normalisation of $P_{M,N}(x)$ on the interval **J**.

$$P_{M,N}(x) = P_{M,N}(s_i) \quad \forall x \in r_i \quad (16)$$

In the case of coupled maps, we are more interested by the distribution of each component x^1, …, x^p of X rather than the distribution of the variable X itself in $\mathbf{J^p}$. We then consider the approximated probability distribution function $P_{\mathbf{N}}(x^j)$ associated to one among several components of $F(X)$ defined by (3) which are one-dimensional maps.

The discrepancies $\boldsymbol{E_1}$ (in norm L_1) and $\boldsymbol{E_2}$ (in norm L_2) between $P_{N_{disc},N_{iter}}(x)$ and the Lebesgue measure which is the invariant measure associated to the symmetric tent map, are defined by

$$E_1(N_{disc},N_{iter}) = \left\| P_{N_{disc},N_{iter}}(x) - 0.5 \right\|_{L_1} \quad (17)$$

$$E_2(N_{disc},N_{iter}) = \left\| P_{N_{disc},N_{iter}}(x) - 0.5 \right\|_{L_2} \quad (18)$$

In the same way an approximation of the correlation distribution function $C_{\mathbf{N}}(x, y)$ is to obtained numerically building a regular partition of M^2 small squares (boxes) of $\mathbf{J^2}$ imbedded in the phase subspace (x^l, x^m)

$$r_{i,j} = [s_i , s_{i+1}[\times [t_j , t_{j+1}[\quad , \; i,j = 0, M-2 \quad (19)$$

$$r_{M-1,j} = [s_{M-1} , 1] \times [t_j , t_{j+1}[\quad , \; j = 0, M-2 \quad (20)$$

$$r_{i,M-1} = [s_i , s_{i+1}[\times [t_{M-1} , 1] \quad , \; i = 0, M-2 \quad (21)$$

$$r_{M-1,M-1} = [s_{M-1} , 1] \times [t_{M-1} , 1] \quad (22)$$

$$s_i = -1 + \frac{2i}{M}, t_j = -1 + \frac{2j}{M}, \; i,j = 0, M \quad (23)$$

the measure of the area of each box is

$$(s_{i+1} - s_i) \cdot (t_{i+1} - t_i) = \left(\frac{2}{M}\right)^2 \quad (24)$$

Once $N + Q$ iterated points $\left(x_n^l, x_n^m\right)$ belonging to these boxes are collected the relative number of iterates with respect to N/M^2 in each box $r_{i,j}$ represents the value $C_{\mathbf{N}}(s_i, t_j)$. The approximated probability distribution function $C_{\mathbf{N}}(x, y)$ defined here is then a *2*-dimensional step function, with M^2 steps. As M can take several values in the next sections, we define

$$C_{M,N}(s_i, t_j) = \frac{1}{4}\frac{M^2}{N}\left(\#r_{i,j}\right) \quad (25)$$

where $\#r_{i,j}$ is the number of iterates belonging to the square $r_{i,j}$ and the constant 1/4 allows the normalisation of $C_{M,N}(x, y)$ on the square $\mathbf{J^2}$.

$$C_{M,N}(x,y) = C_{M,N}(s_i,t_j) \quad \forall (x,y) \in r_{i,j} \quad (26)$$

The discrepancies E_{C_1} in norm L_1 between $C_{N_{disc},N_{iter}}(x, y)$ and the uniform distribution on the square is defined by

$$E_{C_1}(N_{disc},N_{iter}) = \left\| C_{N_{disc},N_{iter}}(x,y) - 0.25 \right\|_{L_1} \quad (27)$$

Finally let $AC_{M,N}(x, y)$ be the autocorrelation distribution function which is the correlation function $C_{M,N}(x, y)$ of (26) defined in the phase space $\left(x_n^l, x_{n+1}^l\right)$ instead of the phase space (x^l, x^m). In order to control that the enhanced chaotic numbers $\left(\overline{x_0}, \overline{x_1}, \overline{x_2}, \cdots, \overline{x_q}, \overline{x_{q+1}}, \cdots\right)$ are uncorrelated, we plot them in the phase subspace $\left(\overline{x_n}, \overline{x_{n+1}}\right)$ and we check if they are uniformly distributed in the square $\mathbf{J^2}$ and if f is concealed .

Fig. 1 shows the values of $E_{AC1}(N_{disc}, NSampl_{iter})$ for a system of *4*-coupled equations when the three components x^1 , x^2 , x^3 are mixed and sampled by x^4 for the threshold values $T_1 = 0.98$, $T_2 = 0.987$, $T_3 = 0.994$ or $T_1 = 0.998$, $T_2 = 0.9987$, $T_3 = 0.9994$.

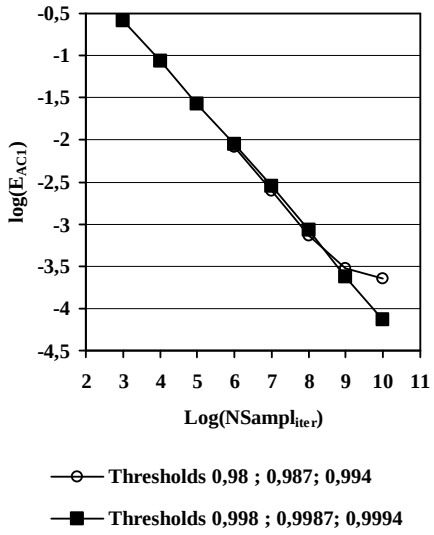

Figure 1. Error of $E_{AC_1}(N_{disc}, NSampl_{iter})$ $N_{\text{disc}}=10^2\times10^2$, $NSampl_{\text{iter}}= 10^3$ to 10^{10}, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1=10^{-14}$.

N_{iter}	$NSampl_{\text{iter}}$	$E_{AC_1}(N_{disc}, NSampl_{iter})$ **4-coupled equation** $T_1 = 0.998$, $T_2 = 0.9987$, $T_3 = 0.9994$
10^5	**93**	**0.68924731**
10^6	**1015**	**0.25881773**
10^7	**10,139**	**0.086706776**
10^8	**100,465**	**0.026815309**
10^9	**1,000,549**	**0.0089111078**
10^{10}	**9,998,814**	**0.0027932033**
10^{11}	**100,001,892**	**0.00085967214**
10^{12}	**999,945,728**	**0.0002346851**
10^{13}	**10,000,046,137**	**0.000073234736**

Table 1. Error of $E_{AC_1}(N_{disc}, NSampl_{iter})$ for a system of 4 coupled-equations when the three components x^1 , x^2 , x^3 are mixed and sampled by x^4 for the threshold values $T_1 = 0.998$, $T_2 = 0.9987$, $T_3 = 0.9994$.

III. DOUBLE TRHESHOLD CHAOTIC SAMPLING

A. *Improved CPRNG*

On can again improve the CPRG previously introduced with respect to the infinity norm instead of the L_1 or L_2 norms because the L_∞ norm is more sensitive than the others to reveal the concealed *f*. For this aim, consider first that in the phase space $\left(x_n^l, x_{n+1}^l\right)$ the graph of the chaotically sampled chaotic numbers is a mix of the graphs of all the $f^{(r)}$ (Fig. 2).

It is obvious as showed on Fig. 3 that for $r = 1$ if $M = 1$ or 2, $AC_{M,N}(x,y)$ is constant and normalized on the square hence $E_{AC\infty}(M,N) = E_{AC1}(M,N) = E_{AC2}(M,N) = 0$.

The autocorrelation function is different from zero only if M > 2 (Fig. 4).

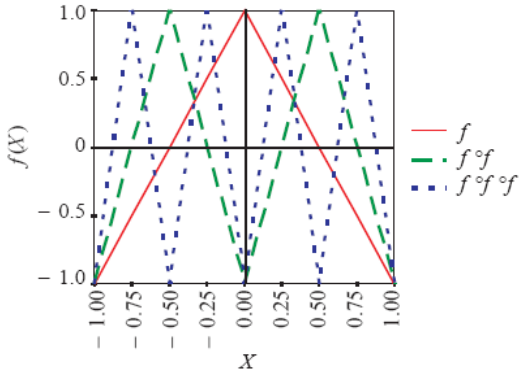

Figure 2. Graphs of the symmetric tent map *f*, $f^{(2)}$ and $f^{(3)}$ on the interval [-1,1].

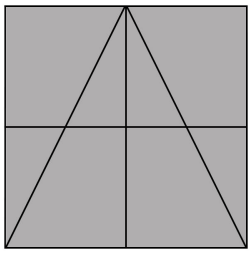

Figure 3. In shaded regions the autocorrelation distribution $AC_{M,N}(x,y)$ is constant for the symmetric tent map *f* on the interval [-1, 1] for $M = 1$ or 2.

In the same way as displayed on Fig. 5, 6 and 7, $E_{AC\infty}(M,N) = E_{AC1}(M,N) = E_{AC2}(M,N) = 0$ for $f^{(i)}$ iff $M < 2^i$. Hence for a given *M*, if we cancel the contribution of all the $f^{(i)}$ for $2^i <$ M, it is not possible to identify the genuine function *f*.

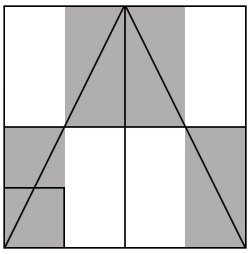

Figure 4. Regions where the autocorrelation distribution $AC_{M,N}(x,y)$ is constant for the symmetric tent map *f* are shaded, for $M = 4$. (The square on the bottom left of the graph shows the size of the $r_{i,j}$ box). $AC_{M,N}(x,y)$ vanishes on the white regions.

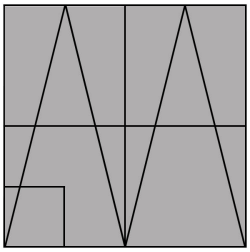

Figure 5. In shaded regions the autocorrelation distribution $AC_{M,N}(x,y)$ is constant for the symmetric tent map $f^{(2)}$ on the interval [-1, 1] for $M = 1$, 2 and 4.

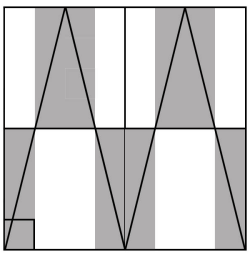

Figure 6. Regions where the autocorrelation distribution $AC_{M,N}(x,y)$ is constant for the symmetric tent map $f^{(2)}$ are shaded for $M = 8$.

B. *Algorithm and Numerical Results*

We describe again the algorithm of the double threshold chaotic sampling in the case of *4*-coupled equations.
Consider the sequence $\left(\overline{x_0}, \overline{x_1}, \overline{x_2}, \cdots, \overline{x_q}, \overline{x_{q+1}}, \ldots\right)$ we want to mix and sample. For each *q-1* there exists $n_{(q-1)}$ in the original sequence. We introduce a second threshold $N' \in \mathbb{N}$ and then we define:

$$\overline{x_q} = \begin{cases} x_n^1 & iff \quad x_n^4 \in \left]T_1, T_2\right[\quad and \quad n - n_{(q-1)} > N' \\ x_n^2 & iff \quad x_n^4 \in \left[T_2, T_3\right[\quad and \quad n - n_{(q-1)} > N' \\ x_n^3 & iff \quad x_n^4 \in \left[T_3, 1\right[\quad and \quad n - n_{(q-1)} > N' \end{cases} \tag{28}$$

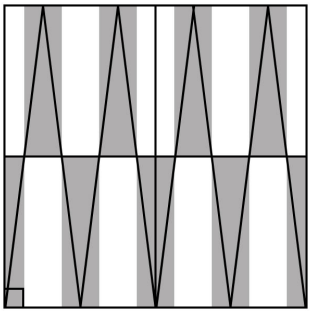

Figure 7. Regions where the autocorrelation distribution $AC_{M,N}(x,y)$ is constant for the symmetric tent map $f^{(3)}$ are shaded for $M = 16$.

As shown previously [9] the errors in L_1 or L_2 norms decrease with the number of chaotic points (as in the law of large numbers) and conversely increase with the number M of boxes used to define $AC_{M,N}(x,y)$. It is the same for the error in L_∞ norm. Fig. 8 shows that when M is greater than 2^5, the sequence defined by (28) behaves better than the one defined by (9).

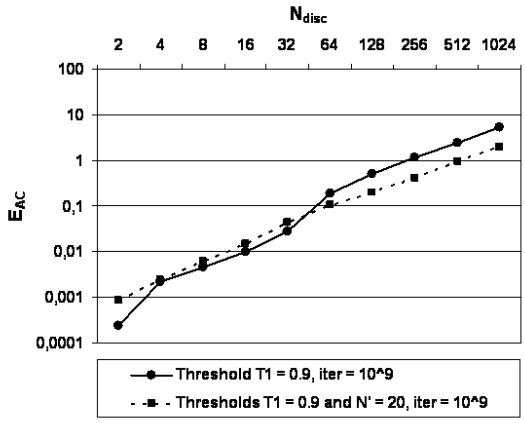

Figure 8. Error of $E_{AC\infty}(N_{disc}, NSampl_{iter})$ $N_{\text{disc}} = 2^1$ to 2^{10}, $NSampl_{\text{iter}} = 10^9$, thresholds T = 0.9 and N' = 20, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$.

Fig. 9 shows that when the number of chaotic points increases the error L_∞ decreases drastically. If N' > 100, it is necessary to use a huge grid of 2^{100}x2^{100} boxes splitting the square $\mathbf{J^2}$ in order to find a trace of the genuine function *f*. This is numerically impossible with double precision numbers. Then the chaotic numbers appear as random numbers.

Others numerical results show the high-potency of theses new CPRNG. Due to limitation of this article, they will be published elsewhere.

IV. CONCLUSION

Using a double threshold in order to sample a chaotic sequence, we have improved with respect to the infinity norm the CPRNG previously introduced. When the value of the second threshold N' is greater than 100, it is impossible to find the genuine function used to generate the chaotic numbers. The new CPRNG family is robust versus the choice of the weak parameter of the system for $10^{-14} < \varepsilon < 10^{-5}$, allowing the use of this family in several applications as for example chaotic cryptography.

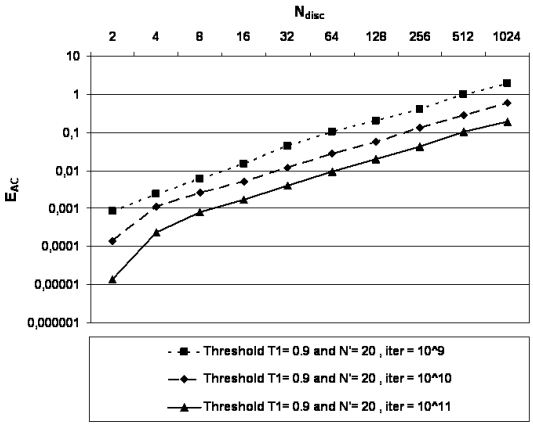

Figure 9. Error of $E_{AC\infty}(N_{disc}, NSampl_{iter})$ $N_{\text{disc}} = 2^1$ to 2^{10}, $NSampl_{\text{iter}} = 10^9$ to 10^{11}, thresholds T = 0.9 and N' = 20, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$.

REFERENCES

[1] Petersen, M. V., Sorensen, H. M., Method of generating pseudo-random numbers in an electronic device, and a method of encrypting and decrypting electronic data. *United States Patent* 7170997, 2007.

[2] Ruggiero, D., Mascolo, D., Pedaci, I., Amato, P., Method of generating successions of pseudo-random bits or numbers. *United States Patent Application* 20060251250, 2006.

[3] S. Hénaff, I. Taralova, R. Lozi, Observers design for a new weakly coupled map function, preprint. http://hal.archives-ouvertes.fr/hal-00368576/fr/

[4] S. Hénaff, I. Taralova, R. Lozi, Dynamical Analysis of a new statistically highly performant deterministic function for chaotic signals generation, preprint. http://hal.archives-ouvertes.fr/hal-00368844/fr/

[5] O. E., Lanford III, Some informal remarks on the orbit structure of discrete approximations to chaotic maps. *Experimental Mathematics*, Vol. 7, 4, 317-324, 1998.

[6] Gora, P., Boyarsky, A., Islam, Md. S., Bahsoun, W., Absolutely continuous invariant measures that cannot be observed experimentally. *SIAM J. Appl. Dyn. Syst.*, 5:1, 84-90 (electronic), 2006.

[7] Lozi, R., Giga-Periodic Orbits for Weakly Coupled Tent and Logistic Discretized Maps. International Conference on Industrial and Applied Mathematics, New Delhi, december 2004, *Modern Mathematical Models, Methods and Algorithms for Real World Systems*, A.H. Siddiqi, I.S. Duff and O. Christensen (Editors), Anamaya Publishers, New Delhi, India pp. 80-124, 2006.

[8] Sprott, J. C., *Chaos and Time-Series Analysis.* Oxford University Press, Oxford, UK, 2003.

[9] R. Lozi, New Enhanced Chaotic Number Generators, *Indian Journal of Industrial and Applied Mathematics*, vol.1, No.1, pp.1-23, 2008.